

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPL. NO.: 09/978,224

APPLICANT: REUBEN BAHAR

FILED: 02/13/2003

FOR: "METHOD AND SYSTEM  
CONFIRMING PROPER  
RECEIPT OF E-MAIL  
TRANSMITTED VIA A  
COMMUNICATIONS  
NETWORK"

Art Unit 2143

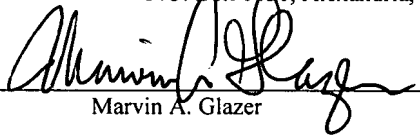
Examiner: Asghar H. Bilgrami

Confirmation No. 4472

Attorney Docket No. 6589-7

**Certificate of Transmission under 37 CFR 1.8**

I hereby certify that this correspondence is being deposited on the date indicated below by first class mail, in the United States Postal Service addressed to: Commissioner of Patents,  
P.O. Box 1450, Alexandria, VA 22313-1450

  
Marvin A. Glazer

10/24/2007  
Date

**BRIEF OF APPELLANT**

MAIL STOP AF  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This Brief is in support of the Notice of Appeal filed in the Patent Office by the above identified Applicant/Appellant on August 6, 2007, appealing the final rejection of the Examiner

1 dated June 6, 2007, finally rejecting claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-  
2 255, 258-271, 279, 288-317, 327-340, and 346-348<sup>1</sup>. A check is enclosed in payment of the fee of  
3 \$255.00 for filing the Appeal Brief, as set forth in § 41.20(b)(2) for a small entity. Also enclosed is  
4 a Petition for One-Month Extension of Time for filing the Appeal Brief, and the enclosed check  
5 includes payment of the related extension fee by a small entity. The Patent Office is hereby  
6 authorized to charge any additional fees required by this paper to Deposit Account No. 03-0088.

7 This Appeal Brief sets forth the authorities and arguments on which Appellant relies to  
8 maintain this appeal. A Claims Appendix, setting forth the text of the claims involved in this  
9 appeal, is attached hereto. Also attached are appendices for evidence and related proceedings.

10  
11 **1. Real Party In Interest.**

12 The real party in interest is the applicant/inventor, namely, Reuben Bahar of West Hills,  
13 California. The claimed invention has not been assigned or licensed.

14  
15 **2. Related Appeals and Interferences.**

16 None.

17  
18  
19  
20  
21 

---

<sup>1</sup> In partial response to the final Office Action mailed June 6, 2007, Applicant canceled claims  
22 155, 157-161, 163-182, 235, 244-247, 256-257, 272-278, 280-287, 318-326, and 341-345 by submitting  
23 an Amendment After Final Office Action, without prejudice to the presentation of such claims in a  
24 continuing application for further prosecution, in order to place the present application in better form  
25 for purposes of appeal. The Examiner confirmed entry of such Amendment on September 6, 2007 via  
26 an Advisory Office Action. While preparing this Appeal Brief, Applicant realized that dependent claims  
27 288-317 should also have been canceled, as they depend from canceled claims; accordingly, on October  
23, 2007, Applicant filed (via facsimile) a Supplemental Amendment After Final Office Action  
canceling dependent claims 288-317.

1 **3. Status of Claims.**

2 None of the pending claims are allowed or objected to. All of claims 1-348 are either: 1)  
3 rejected and being appealed; or 2) canceled, in accordance with the listing below:

<u>Claims</u>	<u>Status</u>
1-183	Canceled.
184-189	Rejected and being appealed.
190.	Canceled.
191-213	Rejected and being appealed.
214	Canceled.
215-229	Rejected and being appealed.
230	Canceled.
231-234	Rejected and being appealed.
235	Canceled.
236-243	Rejected and being appealed.
244-247	Canceled.
248-255	Rejected and being appealed.
256-257	Canceled.
258-271	Rejected and being appealed.
272-278	Canceled.
279	Rejected and being appealed.
280-326	Canceled.
327-340	Rejected and being appealed.
341-345	Canceled.
346-348	Rejected and being appealed.

1     **4. Status of Amendments.**

2             On July 30, 2007, Applicant filed an Amendment After Final Office Action. The entry of  
3     the aforementioned amendment (which merely canceled additional claims) was confirmed by the  
4     Examiner within an Advisory Office Action mailed on September 6, 2007.

5             While preparing this Appeal Brief, Applicant realized that dependent claims 288-317  
6     should also have been canceled, since they all depend, directly or indirectly, from canceled claims  
7     (either canceled claim 287 or canceled claim 272). Accordingly, on October 23, 2007, Applicant  
8     filed (via facsimile) a Supplemental Amendment After Final Office Action canceling dependent  
9     claims 288-317, without prejudice to the presentation of such claims in a continuation patent  
10    application. It is not yet known whether the Examiner will enter such Supplemental Amendment,  
11    though entry of such Supplemental Amendment would appear to be proper pursuant to 37 C.F.R.  
12    §41.33(a).

13  
14    **5. Summary of Claimed Subject Matter.**

15            Applicant has set forth below a concise explanation of the subject matter defined in each of  
16    the independent claims (236, 248, 252, 258, 260, 264, and 268) involved in the appeal, including  
17    references to the specification by page and line number, and to the drawings by reference  
18    characters, where appropriate.

19  
20    Claim 236:

21            Claim 236 recites a method for verifying whether an e-mail message 12 sent by a sending  
22    party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message  
23    12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications  
24    network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18). E-mail message 12 is delivered to a  
25    designated recipient e-mail address. The recited method includes the step of detecting an access  
26  
27

1 event (see spec. p. 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1), and prompts  
2 the accessing party 20 to input recipient data (see spec. p. 27, lines 6-23) before allowing the access  
3 to such email message by the accessing party 20; the aforementioned recipient data includes  
4 identifying data related to the accessing party 20. The method of claim 236 also sends recipient  
5 data back to sending party 10 for confirming proper delivery of e-mail message 12 (see spec. p. 23,  
6 lines 3-14, and p. 31, lines 11-15).  
7  
8

9 Claim 248:

10 Claim 248 recites a system for verifying whether an e-mail message 12 sent by a sending  
11 party 10 was accessed by an intended recipient. The system of claim 248 includes a sender  
12 computer 11 connected to a communications network 13 and from which e-mail message 12 is  
13 transmitted (see spec. p. 13, lines 16-18, and p. 14, lines 12-13). The system of claim 248 also  
14 includes a recipient computer 14/21 connected to communications network 13 (see items 14 and 21  
15 in Fig. 1, and see spec. p. 14, line 24 through p. 15, line 14, and p. 16, line 24 through p. 17, line 9);  
16 the recipient computer 14/21 is capable of receiving e-mail message 12 and includes data storage  
17 17/24 for storing received e-mail message 12 (see items 17 and 24 in Fig. 1, and see spec. p. 17,  
18 lines 10-19).  
19  
20

21 The system of claim 248 also includes software (e.g., executable attachment file 12' in Fig.  
22 1) that is capable of detecting an access event (see spec. p. 17, line 20 through p. 18, line 2); upon  
23 detecting such access event, this software 12' prompts accessing party 20 to input recipient data  
24 before allowing access to e-mail message 12 (see spec. p. 27, lines 6-23). The recipient data  
25 inputted by accessing party 20 includes identifying data which identifies the accessing party 20 (e.g.,  
26  
27

1 see spec. p. 27, lines 13-17, and p. 29, lines 14-23) . The system of claim 248 also includes  
2 “means” (e.g., software) for sending recipient data back to sending party 10 for confirming proper  
3 delivery of e-mail message 12 (see item 28 in Fig. 1; items 44 and 45 in Fig. 2, and see Figs. 3 and  
4 4; also see, for example, spec. p. 19, lines 1-11).

7 Claim 252:

8 Claim 252 recites a system for verifying whether an e-mail message sent by a sending party  
9 10 was accessed by an intended recipient. The system of claim 252 includes a sender computer 11  
10 connected to a communications network 13 and from which e-mail message 12 is transmitted (see  
11 spec. p. 13, lines 16-18, and p. 14, lines 12-13). The system of claim 252 also includes a recipient  
12 computer 14/21 connected to communications network 13 (see items 14 and 21 in Fig. 1, and see  
13 spec. p. 14, line 24 through p. 15, line 14, and p. 16, line 24 through p. 17, line 9); the recipient  
14 computer 14/21 is capable of receiving e-mail message 12 and includes data storage 17/24 for  
15 storing received e-mail message 12 (see items 17 and 24 in Fig. 1, and see spec. p. 17, lines 10-19).

17 The system of claim 252 further includes a “means” for recognizing biometric attributes of  
18 an individual (see spec. p. 29, line 14 through p. 30, line 23).

20 The system of claim 252 also includes software capable of detecting an access event (see  
21 spec. p. 17, line 20, through p. 18, line 2) and identifying an individual through utilization of  
22 inputted biometric attributes of said individual (see spec. p. 29, line 14 through p. 30, line 23).

23 Lastly, the system of claim 252 includes “means” (e.g., software) for sending data that  
24 identifies the accessing party back to sending party 10 for confirming proper delivery of the e-mail  
25

1 message 12 (see item 28 in Fig. 1; items 44 and 45 in Fig. 2, and see Figs. 3 and 4; also see, for  
2 example, spec. p. 19, lines 1-11).

3  
4  
5 Claim 258:

6 Claim 258 recites a method for verifying whether an e-mail message 12 sent by a sending  
7 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message  
8 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications  
9 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18), and is delivered to an e-mail  
10 address. The recited method includes the step of detecting an access event (see spec. p. 17, line 20  
11 through p. 18, line 2; and see items 18 and 25 in Fig. 1), and prompts the accessing party 20 to  
12 input recipient data (see spec. p. 27, lines 6-23) before allowing the access to such email message  
13 by the accessing party 20; the aforementioned recipient data includes identifying data associated  
14 with the accessing party 20. The method of claim 258 also sends recipient data back to sending  
15 party 10 for confirming proper delivery of the e-mail message 12 (see spec. p. 23, lines 3-14, and p.  
16 31, lines 11-15).

17  
18  
19  
20 Claim 260:

21 Claim 260 recites a method for verifying whether an e-mail message 12 sent by a sending  
22 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message  
23 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications  
24 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18), and is delivered to a recipient e-  
25 mail address. The recited method includes the step of detecting an access event (see spec. p. 17,  
26  
27

1 line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1). The method of claim 260 includes  
2 the further step of acquiring recipient data, wherein such recipient data is related to biometric  
3 identification of the accessing party 20 (see spec. p. 29, line 14 through p. 30, line 23).  
4

5 The method of claim 260 also sends recipient data back to sending party 10 for confirming  
6 proper delivery of the e-mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).  
7

8 Claim 264:

9 Claim 264 recites a method for verifying whether an e-mail message 12 sent by a sending  
10 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message  
11 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications  
12 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18). E-mail message 12 is delivered to  
13 an e-mail address. The method of claim 264 includes the step of utilizing biometric identification  
14 information to identify a recipient requesting access to the email message (see spec. p. 29, line 14  
15 through p. 30, line 23).  
16  
17

18 The method of claim 264 further includes the step of detecting an access event (see spec. p.  
19 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1). The method of claim 264 also  
20 sends recipient identification data back to sending party 10 for confirming proper delivery of the e-  
21 mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).  
22  
23

24 Claim 268:

25 Claim 268 recites a method for verifying whether an e-mail message 12 sent by a sending  
26 party 10 was accessed by an intended recipient 20. In practicing such method, an e-mail message  
27

1 12 is transmitted from a sender computer 11 to an intended recipient 20 over a communications  
2 network 13 (see spec. p. 12, lines 3-13, and p. 13, lines 16-18), and is delivered to an e-mail  
3 address. The method of claim 268 includes the further step of identifying a recipient requesting  
4 access to e-mail message 12 using biometric identification information associated with such  
5 recipient (see spec. p. 29, line 14 through p. 30, line 23).

7 The method of claim 268 further includes the step of detecting an access event (see spec. p.  
8 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1). The method of claim 268 also  
9 sends recipient identification data back to sending party 10 for confirming proper delivery of the e-  
10 mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).

12  
13 **6. Grounds of Rejection to be Reviewed on Appeal:**

14 a. Did the Patent Examiner error in rejecting claims 184-189, 191-213, 215-229, 231-234,  
15 236-243, 248-255, 258-271, 279, 327-340, and 346-348, as describing subject matter that would  
16 have been obvious to those skilled in the art under 35 U.S.C. Section 103(a) based upon Choi (U.S.  
17 Pat. No. 6,629,131), Flynn (U.S. Pat. No. 6,618,747), and Bisbee (U.S. Pat. No. 5,748,738)?  
18

19  
20 **7. Argument.**

21 **A. The Cited Prior Art.**

22 **Choi (U.S. Patent No. 6,629,131):**

23  
24 The cited '131 patent to Choi describes a method for confirming receipt of an email  
25 message. Choi's method assigns a unique code to an e-mail message sent by a sender, and records  
26 the unique code in a database. This unique code is generated at the sender's end of the  
27

1 transmission and is attached to the e-mail message as a "CGI executive program". Upon access of  
2 the email message by the recipient, Choi's method sends the unique code that was attached to the  
3 message back to the web server of the sender; this step is performed by the automatic execution of  
4 the attached "CGI executive program" executed at the receiver's end when the e-mail message is  
5 received by the receiver. A comparison is made of the unique code received from the CGI  
6 executive program and the unique code previously recorded when the sender first sent the email  
7 message. If the two codes are identical, then confirmation information is sent to the sender  
8 indicating that the email message has been accessed.  
9

10 Flynn (U.S. Patent No. 6,618,747):  
11

12 The cited '747 patent to Flynn discloses a system wherein an intended recipient is notified  
13 that an email message has been posted at a third party web host for such recipient. Notification of  
14 the existence of the posted e-mail is communicated by the third party web host which sends an e-  
15 mail message informing the recipient that an e-mail message is waiting for the recipient at a  
16 specified third party web host URL. Included in this e-mail message is the third party URL address  
17 where the posted message is located. If the intended recipient accesses the message, a confirmation  
18 notice is sent to the sender to confirm that the message was downloaded. Flynn describes the URL  
19 address at which the posted e-mail message is posted on the third party web host as a "unique call  
20 address" (assigned by Flynn's Web Server 24) that provides access to an e-mail message stored at  
21 such unique call address on the third party Web server. When the email message is downloaded by  
22 the requesting party, Flynn's system sends a confirmation of receipt notice that includes the address  
23 to which the email was downloaded, the time it was downloaded, and optionally, a compressed  
24 copy of the original message.  
25  
26  
27

1        Bisbee (U.S. Pat. No. 5,748,738):

2        The cited patent to Bisbee discloses a system for verifying the authenticity of the creator of  
3 an electronic document. An authentication center provides third party verification that a document  
4 is being transmitted by the originator of the document. Bisbee mentions the use by the  
5 Certification Authority of personal identification information, such as biometric information (e.g.,  
6 retina-, finger-, and voice-prints), to identify the document originator.  
7

8  
9        **B.     The Examiner's Rejections:**

10        Within the final Office Action mailed June 6, 2007, the Patent Examiner finally rejected  
11 claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-  
12 348 under Section 103(a). The Examiner rejected such claims as describing subject matter  
13 considered to be unpatentable over Choi (U.S. Pat. No. 6,629,131), Flynn (U.S. Pat. No.  
14 6,618,747), and Bisbee (U.S. Pat. No. 5,748,738).  
15  
16

17  
18        **C.     The Cited Patents Do Not Render Obvious the Appealed Claims:**

19        Claim 236:

20        Claim 236 sets forth a method for verifying whether an e-mail sent by a sending party was  
21 accessed by an intended recipient. The recited method includes the step of "detecting an access  
22 event, and prompting the party associated with said access event to input recipient data prior to  
23 allowing the requested access". Moreover, claim 236 states that the "recipient data" (which the  
24 recipient must input before being allowed to access the e-mail message) includes "identifying data  
25  
26  
27

1 related to the party associated with said requested access". Claim 236 further recites that such  
2 "recipient data" is then sent to confirm proper delivery of the e-mail message.

3 The Patent Examiner rejected claim 236 within paragraph 4 on page 2 of the final Office  
4 Action mailed June 6, 2007. Within such paragraph 4, the Patent Examiner stated the following:  
5

6 "4. As per claims .... 236, .... Choi disclosed a method for verifying whether an e-mail sent  
7 by a sending party was accessed by an intended recipient, said method comprising a) storing  
8 recipient data pertaining to an actual recipient of e-mail in a data file, said stored data file  
9 containing identifying data that identifies actual e-mail recipient and further being  
10 associated with actual recipient's email address (col. 1, lines 36-53); b) transmitting an e-  
11 mail from a send computer to an intended recipient, the sender computer being connected to  
12 a communications network; c) delivering said e-mail to a recipient e-mail address (col. 2,  
13 lines 59-67). However, Choi did not explicitly disclose d) detecting an access event, and  
14 discovering stored data file that is associated with said actual recipient's e-mail address and  
15 (e) sending identifying data contained in said discovered data file for confirming proper  
delivery of said e-mail."

16 Within the Examiner's above-quoted remarks, the Examiner did not address the requirement in  
17 claim 236 for the step of "detecting an access event, *and prompting the party associated with said*  
18 *access event to input recipient data prior to allowing the requested access*". Neither Choi nor  
19 Flynn discloses or suggests this aspect of applicant's invention.

20 The only portion of the final Office Action in which the Examiner addressed the  
21 requirement in claim 236 for "detecting an access event, and prompting the party associated with  
22 said access event to input recipient data prior to allowing the requested access" is in paragraph 17  
23 on page 7 of the final Office Action. In paragraph 17 of the final Office Action, the Patent  
24 Examiner stated the following:  
25  
26  
27

1           “17. Applicant argued that neither Flynn nor Choi, disclose or suggest prompting a  
2 party requesting to access an e-mail to enter recipient data after detecting an access event.

3           As to applicant’s argument examiner introduced Bisbee, which prompts the user to  
4 enter its recipient data (I.E. biometric, password information) to access the event (checking  
5 the e-mail message). Please see rejection on line 4 [ *sic paragraph 4 ?* ] of this office  
6 action.”

7 As will be shown below, the Patent Examiner’s contention that Bisbee prompts a user to enter  
8 recipient data in order to access an e-mail message is incorrect, and unsupported by the Bisbee  
9 disclosure.

10           The Background section of Bisbee (set forth in columns 1 and 2 of the Bisbee patent) is  
11 concerned with the problem of document alteration/document forgery. Later, (in col. 6), Bisbee  
12 talks about preventing the originator from denying the authenticity of the document. These remarks  
13 relate to the identity of the originator of the document, and not to an individual seeking access to  
14 such document.

15           Bisbee proposes that the true identity of the document originator can be verified by use of a  
16 “Token”, as Bisbee explains at col. 4, lines 35-49, as follows:  
17

18           “       As described below, the public/private key is advantageously delivered in the form  
19 of a Token such as an electronic circuit card conforming to the standards of the PC Memory  
20 Card Interface Association (a PCMCIA card or PC Card) **for use in the originator's**  
21 **computer**. In general a Token is a portable transfer device that is used for transporting  
22 keys, or parts of keys. It will be understood that PC Cards are just one form of delivery  
23 mechanism for public/private keys for Applicant's DAS; other kinds of Tokens may also be  
24 used, such as floppy diskettes and Smart Cards. To ensure reliable delivery a service such  
25 as the bonded courier services commonly used to ferry securities between parties could be  
26 used **to deliver the media to the document originator**.” (Emphasis added)  
27

1 At col. 4, line 61, through col. 5, line 4, the Bisbee specification states the following:

2 “ In an additional aspect of Applicant's invention, the public/private key is only  
3 effective when it is used in conjunction with a certificate and personal identification  
4 information such as the *recipient's* biometric information (e.g., retina-, finger-, and voice-  
5 prints) or a personal identification number (PIN) that is assigned to the *recipient* of the card  
6 by the Certification Authority and that may be delivered separate from the originator's card.  
7 Any subsequent transmitter of the document who is required to digitally sign or encrypt the  
8 document would similarly be provided with a respective card and personal identification  
9 information.”

10 Within the text quoted immediately above, Bisbee uses the word "*recipient*" to mean the recipient  
11 of the Token "for use in the originator's computer" (see col. 4, lines 35-49, which describe delivery  
12 of the Token to the "document originator"). See also col. 4, line 60 (".. the reliable delivery of the  
13 Token to the authorized recipient.").

14 Thus, when Bisbee speaks of "personal identification information such as the *recipient's*  
15 biometric information (e.g., retina-, finger-, and voice-prints) or a personal identification number  
16 (PIN) that is assigned *to the recipient of the card* by the Certification Authority", Bisbee is  
17 referring to the "recipient" of the Token and/or PC Card (i.e., the document transmitter/originator),  
18 and not the intended recipient of the document requiring authentication. Indeed, the only portion of  
19 the Bisbee specification that actually discusses the issue of who has the right to access a document  
20 is in col. 10, lines 17-22; that portion of Bisbee is very vague, and it certainly does not disclose or  
21 suggest the step of prompting the accessing party to input recipient data after detecting an access  
22 event, and prior to allowing the requested access.

25 Accordingly, the Examiner's rejection of claim 236 is not supported by the cited references  
26 and should be reversed.

1 Claim 248:

2 Claim 248 recites a system for verifying whether e-mail sent by a sending party was  
3 accessed by an intended recipient, wherein such system includes, among other things, a recipient  
4 computer connected to a communications network and being capable of receiving and storing a  
5 transmitted e-mail message, and software capable of detecting an access event, "... said software  
6 prompts the party associated with said access event to input recipient data prior to allowing the  
7 requested access".  
8

9 Once again, the Patent Examiner's rejection of claim 248 is set forth in paragraph 4 of the  
10 final Office Action, but such paragraph 4 fails to address the requirement within claim 248 for  
11 software capable of detecting an access event and thereafter prompting the accessing party to input  
12 recipient data prior to allowing the requested access.  
13

14 In addition, for the reasons explained above relative to claim 236, the Examiner's remarks  
15 in paragraph 17 of the final Office Action, based upon Bisbee, fail to demonstrate that Bisbee  
16 teaches or suggests software capable of detecting an access event and thereafter prompting the  
17 accessing party to input recipient data prior to allowing the requested access.  
18

19 Accordingly, the Examiner's rejection of claim 248 is not supported by the cited references  
20 and should be reversed.  
21

22 Claim 252:

23 Claim 252 recites a system for verifying whether e-mail sent by a sending party was  
24 accessed by an intended recipient, the system including, among other things, a recipient computer  
25 connected to a communications network and being capable of receiving and storing a transmitted e-  
26  
27

1 mail message; "biometric identification means" for recognizing biometric attributes of an  
2 individual; software capable of detecting an access event and identifying an individual through  
3 utilization of inputted biometric attributes of said individual; and " means" for sending data that  
4 identifies said individual for confirming proper delivery of said e-mail.  
5

6 The Examiner sets forth the basis of the rejection of claim 252 in paragraph 4 of the final  
7 Office Action. While the Examiner concedes that neither Choi nor Flynn explicitly disclose  
8 detecting an individual by utilizing inputted biometric attributes of an individual, the Examiner  
9 contends that "Bisbee disclosed detecting an individual through utilization of inputted biometric  
10 attributes of said individual (col. 1, lines 37-51 & col. 4, lines 36-67)." The Examiner concludes  
11 that "it would have been obvious ... to have incorporated detecting an accessing individual through  
12 utilization of biometric attributes as disclosed by Bisbee ...".  
13

14 However, the Examiner's arguments are not supported by the Bisbee reference. The portion  
15 of Bisbee's specification noted by the Examiner in col. 1 (lines 37-51) are directed to the problem  
16 of authenticating the "transferor" and/or "document's originator". Likewise, as applicant has  
17 explained above, the portion of Bisbee's specification appearing in col. 4, lines 36-67, is directed to  
18 authenticating the document's originator, and not a subsequent recipient of the document.  
19

20 Accordingly, the Examiner's proposed combination of Bisbee with Choi and Flynn  
21 nonetheless fails to provide, or suggest, the invention recited in claim 252.  
22

23 Claim 258:  
24

25 Claim 258 recites a method for verifying whether an e-mail sent by a sending party was  
26 accessed by an intended recipient. The preamble and steps a) and d) of claim 258 are identical to  
27

1 method claim 236 discussed above. Step b) of claim 258 differs from step b) of claim 236 only in  
2 that claim 258 is less specific about where the email message is delivered [“delivering said e-mail  
3 to *an e-mail address*” (claim 258) versus “delivering said e-mail to *a recipient e-mail address*”  
4 (claim 236)].  
5

6 The differences between step c) of claim 258 and step c) recited in claim 236 are  
7 highlighted in the table below:

8 Claim 258	9 Claim 236
10 c) detecting an access event, and 11 prompting the party 12 <i>that requested said access</i> 13 to input recipient data prior to allowing the 14 requested access, said recipient data including 15 identifying data 16 <i>that is associated with the party that</i> <i>requested</i> said access; and	c) detecting an access event, and prompting the party <i>associated with said access event</i> to input recipient data prior to allowing the requested access, said recipient data including identifying data <i>related to the party associated with said</i> <i>requested</i> access; and

17  
18 The Examiner’s asserted basis for rejecting claim 258 is identical to the Examiner’s asserted basis  
19 for rejecting claim 236 already discussed above. Applicant’s remarks, set forth above and directed  
20 to rejected claim 236, apply with equal force relative to the rejection of claim 258. The Patent  
21 Examiner’s contention that Bisbee prompts a user to enter recipient data in order to access an e-  
22 mail message is incorrect, and the rejection of claim 258 should be reversed.  
23  
24  
25  
26  
27

1 Claim 260:

2 Claim 260 recites a method for verifying whether e-mail sent by a sending party was  
3 accessed by an intended recipient, and includes, *inter alia*, the steps of detecting an access event;  
4 acquiring recipient data that is related to biometric identification of the recipient; and sending  
5 recipient data for confirming proper delivery of said e-mail. The Examiner's rejection of claim 260  
6 is set forth in paragraph 4 of the final Office Action. On page 3 of the final Office Action, the  
7 Examiner concedes that the cited patents to Flynn and Choi fail to disclose detecting the identity of  
8 an individual through utilization of inputted biometric attributes of said individual. The Examiner  
9 contends that it would have been obvious to those skilled in the art to apply Bisbee's teachings  
10 regarding biometric attributes to identify the party who received an email message.  
11

12  
13 As noted above, Bisbee's discussion of "personal identification information such as the  
14 *recipient's* biometric information (e.g., retina-, finger-, and voice-prints) ..." refers to the party who  
15 originates and/or transmits a document, who is a "recipient" of the Token and/or PC Card used to  
16 authenticate the sender of the document. Bisbee never states or suggests that biometric  
17 information might be used to identify a party receiving such document.  
18

19 Accordingly, the Examiner's proposed combination of Bisbee with Choi and Flynn fails to  
20 render obvious the subject matter recited in claim 260, and the Examiner's rejection should  
21 therefore be reversed.  
22

23 Claim 264:

24  
25 Claim 264 recites a method for verifying whether e-mail sent by a sending party was  
26 accessed by an intended recipient, including, among others, the steps of identifying a recipient  
27

1 utilizing biometric identification; detecting an access event; and sending data that identifies said  
2 recipient for confirming proper delivery of said e-mail. The Examiner's rejection of claim 264 is  
3 set forth in paragraph 4 of the final Office Action.  
4

5 As noted in regard to claim 260, the Examiner has conceded (see page 3 of the final Office  
6 Action) that the cited patents to Flynn and Choi fail to disclose detecting the identity of an  
7 individual through utilization of inputted biometric attributes of said individual. Nonetheless, the  
8 Examiner contends that it would have been obvious to those skilled in the art, based upon Bisbee,  
9 to utilize biometric attributes to identify the party who received an email message.  
10

11 The applicant has already pointed out that Bisbee's disclosure teaches the use of biometric  
12 information only to identify the originator/sender of a document, and that Bisbee's disclosure fails  
13 to disclose or suggest the use of biometric information to identify a party receiving a document.  
14 Therefore, the Examiner's proposed combination of Bisbee with Choi and Flynn does not suggest  
15 the subject matter recited in claim 264, and the Examiner's rejection should accordingly be  
16 reversed.  
17

18 Claim 268:

19 Claim 268 recites a method for verifying whether an e-mail sent by a sending party was  
20 accessed by an intended recipient. The preamble and steps a), b), d) and e) of claim 268 are  
21 identical to method claim 264 discussed above. The differences between step c) of claim 268 and  
22 step c) recited in claim 264 are highlighted in the table below:  
23  
24  
25  
26  
27

Claim 268	Claim 264
c) identifying a recipient <i>in association with</i> biometric identification;	c) identifying a recipient <i>utilizing</i> biometric identification;

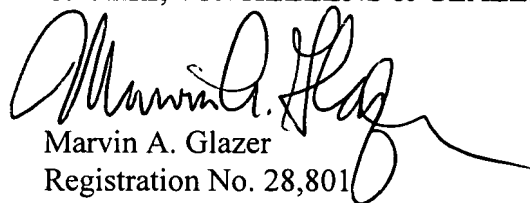
Notwithstanding the differences in the wording of step c) as between claims 268 and 264, the cited Bisbee patent does not make use of any biometric information to identify the recipient of a document. Thus, the rejection of claim 268 should be reversed for essentially the same reasons as explained above in regard to independent claims 260 and 264.

**8. Conclusion:**

Accordingly, Appellant submits that the appealed independent claims 236, 248, 252, 258, 260, 264, and 268, and those appealed claims dependent therefrom, define subject matter that is patentably distinguishable over the applied prior art, and requests the Board to reverse the rejection of appealed claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-348.

Respectfully submitted,

CAHILL, VON HELLENS & GLAZER P.L.C.

  
Marvin A. Glazer  
Registration No. 28,801

155 Park One  
2141 East Highland Avenue  
Phoenix, Arizona 85016  
Ph. (602) 956-7000  
Fax (602) 495-9475  
Docket No. 6589-A-7

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7

4

5

- 6

7

9

0

1

1 and wherein the step of detecting an access event includes the step of executing the first  
2 module of the executable attachment file.

3  
4 189. The method as in claim 188, wherein the executable attachment file has a second module  
5 transmitted and delivered therewith, the second module for detecting the access event, and further  
6 comprising the step of automatically executing the second module upon delivery of the attachment  
7 file to the recipient e-mail address.

8  
9 190. *Canceled.*

10  
11 191. The method as in claim 236, wherein said recipient e-mail address is associated with a  
12 recipient computer.

13  
14 192. The method as in claim 191, wherein said recipient computer is a server of a service  
15 provider.

16  
17 193. The method as in claim 191, wherein said recipient computer is a user system that is  
18 directly accessible by a recipient, said user system including electronic mail processing software.

19 194. The method as in claim 236, wherein said inputted recipient data pertains to  
20 alphanumeric text identification, biometric identification, password identification, a computer  
21 generated user code, or a combination thereof.

22  
23 195. The method as in claim 236, wherein said inputted recipient data comprises identity  
24 information that identifies an individual.

1 196. The method as in claim 195, wherein said identity information pertains to biometric  
2 identification.

3  
4 197. The method as in claim 196 further comprising the step of recognizing biometric  
5 attributes of an individual.

6  
7 198. The method as in claim 195, wherein said identity information includes alphanumeric  
8 text identification information.

9  
10 199. The method as in claim 236 , wherein said inputted recipient data comprises information  
11 that identifies a business.

12  
13 200. The method as in claim 236, wherein said inputted recipient data comprises information  
14 that identifies an organization.

15  
16 201. The method as in claim 236 , wherein said inputted recipient data comprises a computer  
17 generated user code.

18  
19 202. The method as in claim 236 further including the step of sending access event data of  
20 attendant conditions of said access event.

21  
22 203. The method as in claim 236 , wherein said recipient is an individual.

23  
24 204. The method as in claim 236, wherein said recipient is a business.

25  
26 205. The method as in claim 236, wherein said recipient is an organization.

1 206. The method as in claim 236, wherein said inputted recipient data is used to verify proper  
2 delivery of legal documents.

3  
4 207. The method as in claim 236, wherein said inputted recipient data is used to verify  
5 proper delivery of confidential documents.

6  
7 208. The method recited by claim 260 wherein said step of sending recipient data for  
8 confirming proper delivery of said e-mail includes the steps of:

9 a) generating a confirmation of receipt notice wherein the acquired recipient data is  
10 included with said confirmation of receipt notice; and

11 b) sending said confirmation of receipt notice, wherein the acquired recipient data  
12 contained with said confirmation of receipt notice can be compared to information associated with  
13 said intended recipient in order to verify whether the email was accessed by the intended recipient.

14  
15 209. The method as in claim 260, wherein said access event comprises access of said e-mail  
16 that was delivered to said recipient e-mail address.

17  
18 210. The method as in claim 260, wherein said access event comprises access of an e-mail  
19 account associated with said recipient e-mail address.

20  
21 211. The method as in claim 260, wherein said access event comprises activation of e-mail  
22 processing software associated with said recipient e-mail address.

23  
24 212. The method as in claim 260, wherein the step of transmitting an e-mail from a sender  
25 computer includes attaching an executable attachment file in conjunction with the e-mail, the  
26

1 executable attachment file having a first module for acquiring recipient data that is related to  
2 biometric identification of the recipient, and

3 wherein the step of detecting an access event includes the step of executing the first module  
4 of the executable attachment file.

5  
6 213. The method as in claim 212, wherein the executable attachment file has a second module  
7 transmitted and delivered therewith, the second module for detecting the access event, and further  
8 comprising the step of:

9 automatically executing the second module upon delivery of the attachment file to the  
10 recipient e-mail address.

11  
12 214. Canceled.

13  
14 215. The method as in claim ~~208~~ 260, wherein said recipient e-mail address is associated  
15 with a recipient computer.

16  
17 216. The method as in claim 215, wherein said recipient computer is a server of a service  
18 provider that is capable of receiving e-mail.

19  
20 217. The method as in claim 215, wherein said recipient computer is a user system that is  
21 directly accessible by the recipient, said user system including electronic mail processing software  
22 and being capable of receiving e-mail.

23  
24 218. The method as in claim 260, wherein said acquired recipient data is related to a  
25 biometric imprint, alphanumeric text identification, password identification, a computer generated  
26

1 user code, or a combination thereof.

2  
3 219. The method as in claim 260, wherein said acquired recipient data comprises identity  
4 information that identifies an individual.

5  
6 220. The method as in claim 260 further comprising means for recognizing biometric  
7 attributes of an individual.

8  
9 221. The method as in claim 260, wherein said acquired recipient data comprises  
10 information that identifies a business.

11  
12 222. The method as in claim 260, wherein said acquired recipient data comprises  
13 information that identifies an organization.

14  
15 223. The method as in claim 260, wherein said acquired recipient data comprises a  
16 computer generated user code.

17  
18 224. The method as in claim 260 further including the step of sending access event data  
19 of conditions attendant said access event.

20  
21 225. The method as in claim 260, wherein said recipient is an individual.

22  
23 226. The method as in claim 260, wherein said recipient is a business.

24  
25 227. The method as in claim 260, wherein said recipient is an organization.

1 228. The method as in claim 260, wherein said sent recipient data is used to verify proper  
2 delivery of legal documents.

3  
4 229. The method as in claim 260, wherein said sent recipient data is used to verify proper  
5 delivery of confidential documents.

6  
7 230. Canceled.

8  
9 231. The method as in claim 260, wherein said recipient data is acquired as a requisite  
10 condition for permitting access to said delivered e-mail.

11  
12 232. The method as in claim 260, wherein said recipient data is acquired as a requisite  
13 condition for permitting access to said recipient e-mail address.

14  
15 233. The method as in claim 260, wherein said recipient data is acquired as a requisite  
16 condition for operating a remote user computer, said remote user computer being operable to gain  
17 access to said recipient e-mail address.

18  
19 234. The method as in claim 260, wherein said recipient data is comprised of  
20 alphanumeric text, said alphanumeric text being associated with the at least one biometric attribute  
21 of said recipient.

22  
23 235. Canceled.

24  
25 236. A method for verifying whether an e-mail sent by a sending party was accessed by  
26 an intended recipient, said method comprising:

- 1 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
2 computer being connected to a communications network;  
3 b) delivering said e-mail to a recipient e-mail address;  
4 c) detecting an access event, and prompting the party associated with said access event to  
5 input recipient data prior to allowing the requested access, said recipient data including identifying  
6 data related to the party associated with said requested access; and  
7 d) sending recipient data for confirming proper delivery of said e-mail.  
8

9 237. The method recited by claim 264 wherein the step of sending data that identifies said  
10 recipient for confirming proper delivery of said e-mail includes the steps of :

- 11 a) generating a confirmation of receipt notice wherein the data that identifies the recipient  
12 is included with said confirmation of receipt notice; and  
13 b) sending said confirmation of receipt notice, wherein the data that identifies the recipient  
14 that is included with said confirmation of receipt notice can be compared to information associated  
15 with said intended recipient in order to verify whether the email was accessed by the intended  
16 recipient.  
17

18 238. The method as in claim 264, wherein said data that identifies said recipient is related  
19 to a biometric imprint, alphanumeric text identification, password identification, a computer  
20 generated user code, or a combination thereof.  
21

22 239. The method as in claim 264, wherein the data that identifies said recipient is  
23 comprised of alphanumeric text, said alphanumeric text being associated with ~~the~~ at least one  
24 biometric attribute of said recipient.  
25  
26  
27

1 240. The method as in claim 264 further including the step of recognizing biometric  
2 attributes of an individual.

3 241. The method as in claim 264, wherein said data that identifies said recipient  
4 comprises identity information that identifies an individual.

5  
6 242. The method as in claim 264, wherein said data that identifies said recipient  
7 comprises information that identifies a business.

8  
9 243. The method as in claim 264, wherein said data that identifies said recipient  
10 comprises information that identifies an organization.

11  
12 244. - 247. Canceled.

13  
14 248. A system for verifying whether e-mail sent by a sending party was accessed by an  
15 intended recipient, said system comprising:

16 a) a sender computer connected to a communications network and from which an e-  
17 mail is transmitted;

18 b) a recipient computer connected to said communications network, said recipient  
19 computer capable of receiving said transmitted e-mail and further having data storage means for  
20 storing said received e-mail;

21 c) software capable of detecting an access event, wherein, upon detecting said access  
22 event, said software prompts the party associated with said access event to input recipient data prior  
23 to allowing the requested access, said recipient data comprising identifying data related to the party  
24 associated with said requested access; and

25 d) means for sending recipient data for confirming proper delivery of said e-mail.  
26  
27

1 249. The system as in claim 248, wherein said access event comprises access of a delivered e-  
2 mail.

4 250. The system as in claim 248, wherein said access event comprises access of an e-mail  
5 account associated with the e-mail address to which said e-mail was delivered.

7 251. The system as in claim 248, wherein said access event comprises activation of the e-  
8 mail processing software associated with the e-mail address to which said e-mail was delivered.

10 252. A system for verifying whether e-mail sent by a sending party was accessed by an  
11 intended recipient, said system comprising:

12 a) a sender computer connected to a communications network and from which an e-mail is  
13 transmitted;

14 b) a recipient computer connected to said communications network, said recipient  
15 computer being capable of receiving said transmitted e-mail and further having data storage means  
16 for storing said received e-mail;

17 c) biometric identification means for recognizing biometric attributes of an individual;

18 d) software capable of detecting an access event and identifying an individual through  
19 utilization of inputted biometric attributes of said individual; and

20 e) means for sending data that identifies said individual for confirming proper delivery of  
21 said e-mail.

23 253. The system as in claim 252, wherein said access event comprises access of a  
24 delivered e-mail.

1 254. The system as in claim 252, wherein said access event comprises access of an e-mail  
2 account associated with the e-mail address to which said e-mail was delivered.

3  
4 255. The system as in claim 252, wherein said access event comprises activation of the e-mail  
5 processing software associated with the e-mail address to which said e-mail was delivered.

6  
7 256. - 257. Canceled.

8  
9 258. A method for verifying whether an e-mail sent by a sending party was accessed by an  
10 intended recipient, said method comprising:

11 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
12 computer being connected to a communications network;

13 b) delivering said e-mail to an e-mail address;

14 c) detecting an access event, and prompting the party that requested said access to input  
15 recipient data prior to allowing the requested access, said recipient data including identifying data  
16 that is associated with the party that requested said access; and

17 d) sending recipient data for confirming proper delivery of said e-mail.

18  
19 259. The method recited by claim 236 wherein said step of sending recipient data for confirming  
20 proper delivery of said e-mail includes the steps of:

21 a) generating a confirmation of receipt notice wherein the inputted recipient data is included  
22 with said confirmation of receipt notice; and

23 b) sending said confirmation of receipt notice, wherein the inputted recipient data included  
24 with said confirmation of receipt notice can be compared to information associated with said  
25 intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

1 260. A method for verifying whether e-mail sent by a sending party was accessed by an  
2 intended recipient, said method comprising:

- 3 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
4 computer being connected to a communications network;  
5 b) delivering said e-mail to a recipient e-mail address;  
6 c) detecting an access event;  
7 d) acquiring recipient data that is related to biometric identification of the recipient; and  
8 e) sending recipient data for confirming proper delivery of said e-mail.  
9

10 261. The method as recited in claim 260 wherein said recipient data is acquired prior to said  
11 access event.  
12

13 262. The method as recited in claim 260 wherein said recipient data is acquired after said access  
14 event.  
15

16 263. The method as recited in claim 260 wherein said recipient data is sent to an e-mail address.  
17

18 264. A method for verifying whether e-mail sent by a sending party was accessed by an  
19 intended recipient, said method comprising:

- 20 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
21 computer being connected to a communications network;  
22 b) delivering said e-mail to an e-mail address;  
23 c) identifying a recipient utilizing biometric identification;  
24 d) detecting an access event; and  
25 e) sending data that identifies said recipient for confirming proper delivery of said e-mail.  
26  
27

1 265. The method as recited in claim 264 wherein said recipient is identified prior to said access event.

2  
3 266. The method as recited in claim 264 wherein said recipient is identified after said access  
4 event.

5  
6 267. The method as recited in claim 264 wherein said data that identifies said recipient is sent to  
7 an e-mail address.

8  
9 268. A method for verifying whether e-mail sent by a sending party was accessed by an intended  
10 recipient, said method comprising:

- 11 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
12 computer being connected to a communications network;  
13 b) delivering said e-mail to an e-mail address;  
14 c) identifying a recipient in association with biometric identification;  
15 d) detecting an access event; and  
16 e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

17  
18 269. The method as in claim 268 wherein said recipient is identified prior to said access event.

19  
20 270. The method as in claim 268 wherein said recipient is identified after said access event.

21  
22 271. The method as in claim 268 wherein said data that identifies said recipient is sent to an e-  
23 mail address.

24  
25 272. - 278. Canceled.

1 279. The system as in claim 252, wherein said data that identifies said individual for confirming  
2 proper delivery of said e-mail is sent to an e-mail address.

3  
4 280. - 326. Canceled.

5  
6 327. The method as in claim 236, wherein said recipient data for confirming proper delivery of  
7 said e-mail is sent to an e-mail address.

8  
9 328. The method as in claim 236, wherein a remote user computer may be used to gain remote  
10 access to said recipient e-mail address.

11  
12 329. The method as in claim 236 wherein the party that is associated with said access event is  
13 an individual.

14  
15 330. The method as in claim 236 wherein the party that is associated with said access event is a  
16 business.

17  
18 331. The method as in claim 236 wherein the party that is associated with said access event is  
19 an organization.

20  
21 332. The method as in claim 258 wherein said recipient data for confirming proper delivery of  
22 said e-mail is sent to an e-mail address.

23  
24 333. The method as in claim 184, wherein said confirmation of receipt notice is sent to an e-  
25 mail address.

1 334. The method as in claim 258, wherein said inputted recipient data pertains to alphanumeric  
2 text identification, biometric identification, password identification, a computer generated user  
3 code, or a combination thereof.

4  
5 335. The method as in claim 208, wherein said confirmation of receipt notice is sent to an e-  
6 mail address.

7  
8 336. The method as in claim 260, wherein a remote user computer may be used to gain remote  
9 access to said recipient e-mail address.

10  
11 337. The method as in claim 219, wherein said identity information includes alphanumeric text  
12 identification.

13  
14 338. The method as in claim 237, wherein said confirmation of receipt notice is sent to an e-  
15 mail address.

16  
17 339. The method as in claim 268 , wherein said data that identifies said recipient is related to a  
18 biometric imprint, alphanumeric text identification, password identification, a computer generated  
19 user code, or a combination thereof.

20  
21 340. The method as in claim 268 further comprising the step of recognizing biometric attributes  
22 of an individual.

23  
24 341. - 345. Canceled.

1 346. The system as in claim 248, wherein said recipient data for confirming proper delivery of  
2 said e-mail is sent to an e-mail address.

3  
4 347. The system as in claim 252, wherein said individual is identified prior to said access event.

5  
6 348. The system as in claim 252, wherein said individual is identified after said access event.  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

1 **EVIDENCE APPENDIX**

2 In regard to this Appeal, Appellant does not rely upon any evidence submitted pursuant to  
3 37 C.F.R. §§ 1.130, 1.131 or 1.132.

4 The Patent Examiner has relied upon U.S. Pat. No. 6,629,131 (Choi); U.S. Pat. No.  
5 6,618,747 (Flynn), and U.S. Pat. No. 5,748,738 (Bisbee), and Appellant has included remarks in the  
6 attached Brief directed to such patent references. Accordingly, copies of the Choi, Flynn, and  
7 Bisbee patents are attached hereto for the convenience of the Board.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27

- 38 -